

Random subgroups of acylindrically hyperbolic groups and hyperbolic embeddings

Joseph Maher and Alessandro Sisto

January 3, 2017

Abstract

Let G be an acylindrically hyperbolic group. We consider a random subgroup H in G , generated by a finite collection of independent random walks. We show that, with asymptotic probability one, such a random subgroup H of G is a free group, and the semidirect product of H acting on $E(G)$ is hyperbolically embedded in G , where $E(G)$ is the unique maximal finite normal subgroup of G .

Contents

1	Introduction	2
1.1	Acknowledgments	4
2	Background and main theorem	4
2.1	Hyperbolically embedded subgroups	7
2.2	Outline	8
2.3	Notation and standing assumptions	10
3	Estimates for random walks	11
3.1	Exponential decay	11
3.2	Matching	12
4	Schottky groups	14
5	Special case: one generator	19
5.1	Asymmetric elements	19
5.2	Random elements are asymmetric	22
6	General case: many generators	26

1 Introduction

Acylically hyperbolic groups have been defined by Osin, who showed in [Osi16] that several approaches to groups that exhibit rank one behaviour [BF02, Ham08, DGO11, Sis16b] are all equivalent; see Section 2 for the precise definition. Acylindrically hyperbolic groups form a very large class of groups that vastly generalises the class of non-elementary hyperbolic groups and includes non-elementary relatively hyperbolic groups, mapping class groups [MM99, Bow06, PS16], $\text{Out}(F_n)$ [BF14], many groups acting on $\text{CAT}(0)$ spaces [BHS14, CM16, Gen16, Hea16, Sis16b], and many others, see for example [GS16, MO15, Osi15].

Acylindrical hyperbolicity has strong consequences: For example, every acylindrically hyperbolic group is SQ-universal (in particular it has uncountably many pairwise non-isomorphic quotients) and its bounded cohomology is infinite dimensional in degrees 2 [HO13] and 3 [FPS15]. These results all rely on the notion of *hyperbolically embedded subgroup*, as defined in [DGO11] (see Section 2 for the definition), and in fact, on virtually free hyperbolically embedded subgroups. Hyperbolically embedded subgroups are hence very important for the study of acylindrically hyperbolic groups, and in fact they enjoy several nice properties such as almost malnormality [DGO11] and quasiconvexity [Sis16a].

In this paper we show that, roughly speaking, a random subgroup H of an acylindrically hyperbolic group is free and virtually hyperbolically embedded. We now give a slightly simplified version of our main theorem, see Section 2 for a more refined statement. We shall write $E(G)$ for the maximal finite normal subgroup of G , which for G acylindrically hyperbolic exists by [DGO11, Theorem 6.14], and given a subgroup $H < G$, we shall write $HE(G)$ for the subset of G consisting of $\{hg \mid h \in H, g \in E(G)\}$, which in this case is a subgroup, as $E(G)$ is normal. We say that a property P holds with *asymptotic probability one* if the probability P holds tends to one as n tends to infinity.

Theorem 1. *Let G be an acylindrically hyperbolic group, with maximal finite normal subgroup $E(G)$, and let μ be a probability measure on G whose support is finite and generates G as a semigroup. For k, n positive integers, let $H_{k,n}$ denote the subgroup of G generated by k independent random walks generated by μ , each of length n , which we shall denote by $w_{i,n}$.*

Then for each fixed k , the probability that each of the following events occurs with asymptotic probability one.

1. *The subgroup H is freely generated by the $\{w_{1,n_1}, \dots, w_{k,n_k}\}$ and quasi-isometrically embedded.*

2. *The subgroup $HE(G)$ is a semidirect product $H \rtimes E(G)$, and is hyperbolically embedded in G .*

The first part of Theorem 1 was previously shown by Taylor and Tiozzo [TT16], and they apply this result to study random free group and surface group extensions. The second part is definitely the main contribution of this paper. For the experts, we note that we can fix the generating set with respect to which $H \rtimes E(G)$ is hyperbolically embedded, see Theorem 8.

The study of generic properties of groups in geometric group theory goes back at least to Gromov [Gro87, Gro03], and we make no attempt to survey the substantial literature on this topic, see for example [GMO10] for a more thorough discussion, though we now briefly mention some closely related results. This model of random subgroups is used in Guivarc'h's [Gui90] proof of the Tits alternative for linear groups, and is also developed by Rivin [Riv10] and Aoun [Aou11], who proves that a random subgroup of a non-virtually solvable linear group is free and undistorted. Gilman, Miasnikov and Osin [GMO10] consider subgroups of hyperbolic groups generated by k elements arising from nearest neighbour random walks on the corresponding Cayley graph, and they show that the probability that the resulting group is a quasi-isometrically embedded free group, freely generated by the k unreduced words of length n , tends to one exponentially quickly in n . The fact that the k elements freely generate a free group as n becomes large was shown earlier for free groups by Jitsukawa [Jit02] and Martino, Turner and Ventura, [MTV], and for braid groups by Miasnikov and Ushakov [MU08]. Our argument makes use of particular group elements which we call strongly asymmetric, namely loxodromic elements g contained in maximal cyclic subgroups which are equal to $\langle g \rangle \rtimes E(G)$. We say a loxodromic element g is weakly asymmetric if it is contained in a maximal cyclic subgroup which is a semidirect product $\langle g \rangle \rtimes E(G)$, see Section 2 for full details. Masai [Mas14] has previously shown that random elements of the mapping class group are strongly asymmetric, and the argument we present uses similar methods in the context of acylindrically hyperbolic groups. Mapping class groups have trivial maximal finite normal subgroups, except for a finite list of surfaces in which $E(G)$ is central, see for example [FM12, Section 3.4], so in the case of the mapping class groups there is no distinction between weakly and strongly asymmetric elements.

Theorem 1 is used in [HS16] to study the bounded cohomology of acylindrically hyperbolic groups.

1.1 Acknowledgments

The first author acknowledges the support of PSC-CUNY and the Simons Foundation.

This material is based upon work supported by the National Science Foundation under Grant No. DMS-1440140 while the authors were in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Fall 2016 semester.

2 Background and main theorem

We say a geodesic metric space (X, d_X) , which need not be proper, is *Gromov hyperbolic*, δ -*hyperbolic* or just *hyperbolic*, if there is a number $\delta \geq 0$ for which every geodesic triangle in X satisfies the δ -*slim triangle* condition, i.e. for any geodesic triangle, any side is contained in the δ -neighbourhood of the other two sides.

Let G be a countable group which acts on a hyperbolic space X by isometries. We say the action of G on X is *non-elementary* if G contains two hyperbolic elements with disjoint pairs of fixed points at infinity. We say a group G acts *acylindrically* on a Gromov hyperbolic space X , if there are real valued functions R and N such that for every number $K \geq 0$, and for any pair of points x and y in X with $d_X(x, y) \geq R(K)$, there are at most $N(K)$ group elements g in G such that $d_X(x, gx) \leq K$ and $d_X(y, gy) \leq K$. We shall refer to R and N as the *acylindricity functions* for the action. This definition is due to Sela [Sel97] for trees, and Bowditch [Bow06] for general metric spaces.

We say a group G acts *acylindrically hyperbolically* on a space X , if X is hyperbolic, and the action is non-elementary and acylindrical. A group is *acylindrically hyperbolic* if it admits an acylindrically hyperbolic action on some space X .

A finitely generated subgroup H in G is *quasi-isometrically embedded* in X , if for any choice of word metric d_H , and any basepoint $x_0 \in X$, there are constants K and c such that for any two elements h_1 and h_2 in H ,

$$\frac{1}{K}d_X(h_1x_0, h_2x_0) - c \leq d_H(h_1, h_2) \leq Kd_X(h_1x_0, h_2x_0) + c.$$

We say that a subgroup H of G is *geometrically separated* in X , if for each $x_0 \in X$ and $R \geq 0$ there exists $B(R)$ so that for each $g \in G \setminus H$, we have that the diameter of $N_R(gHx_0) \cap N_R(Hx_0)$ is bounded by B , where N_R denotes the metric R -neighborhood in X .

For the remainder of this paper fix an acylindrically hyperbolic group G . We shall write $E(G)$ for the maximal finite normal subgroup of G ,

which exists and is unique by [DGO11, Theorem 6.14]. Given an element $g \in G$, let $E(g)$ be the maximal virtually cyclic subgroup containing g , which is well-defined by work of Bestvina and Fujiwara [BF02]. For a hyperbolic element g , let $\Lambda(g) = \{\lambda_+(g), \lambda(g)\}$ be the set consisting of the pair of attracting and repelling fixed points for g in ∂X . We shall write $\text{stab}(\Lambda(g))$ for the stabilizer of this set in G . Dahmani, Guirardel and Osin [DGO11, Corollary 6.6] show that in fact

$$E(g) = \text{stab}(\Lambda(g)).$$

For any hyperbolic element g , the group $E(g)$ is always quasi-isometrically embedded and geometrically separated.

The subgroup $E(G)$ acts trivially on the Gromov boundary ∂X , so in many applications it may be natural to consider $G/E(G)$, which will have a trivial maximal finite subgroup, and a reader interested in this case should feel free to assume $E(G)$ is trivial, which simplifies the arguments and statements in many places. We shall write $\langle g_1, \dots, g_k \rangle$ for the subgroup of H generated by $\{g_1, \dots, g_k\}$, and in particular, $\langle g \rangle$ denotes the cyclic group generated by g . Recall that given a subgroup $H < G$, we will write $HE(G)$ for the subset of G consisting of $\{hg \mid h \in H, g \in E(G)\}$, which is a subgroup, as $E(G)$ is normal. If $H \cap E(G) = \{1\}$, then the group $HE(G)$ is a finite extension of H by $E(G)$, but in general need not be either a product $H \times E(G)$, or a semidirect product, which we shall write as $H \ltimes E(G)$. The following observation is elementary, but we record it as a proposition for future reference.

Proposition 2. *Let G be a countable group acting acylindrically hyperbolically on X , and let H be a subgroup of G with trivial intersection with $E(G)$, i.e. $H \cap E(G) = \{1\}$. Then the subgroup $HE(G)$ is a semidirect product $H \ltimes E(G)$.*

Proof. The quotient $(HE(G))/E(G)$ corresponds to the set of cosets $hE(G)$. If h is a non-trivial element of H then $hE(G) \neq E(G)$, as $H \cap E(G) = \{1\}$. Therefore, $(HE(G))/E(G)$ is isomorphic to H , and the inclusion of H into $HE(G)$ gives a section $H \rightarrow HE(G)$, i.e. a homomorphism whose composition with the quotient map is the identity on H . This implies that $HE(G)$ is a split extension of $(HE(G))/E(G)$ by $E(G)$, and hence a semidirect product $H \ltimes E(G)$. \square

If g is a hyperbolic element, then $\langle g \rangle$ is an infinite cyclic group, and the subgroup $E(g)$ always contains $\langle g \rangle E(G) = \langle g \rangle \ltimes E(G)$, but may be larger. For example, $E(g) = E(g^2)$ but $E(g^2)$ cannot be equal to $\langle g^2 \rangle E(G)$, as $E(g)$ contains g . Furthermore, the subgroup $\langle g^2 \rangle E(G)$ is quasi-isometrically embedded, but not geometrically separated, as g

coarsely stabilizes this subgroup. We say that a group element $g \in G$ is *weakly asymmetric* if $E(g)$ is equal to $\langle g \rangle \times E(G)$, and *strongly asymmetric* when $E(g)$ is actually the product $\langle g \rangle \times E(G)$. Strongly asymmetric elements are sometimes called special, though we do not use this terminology in this paper. We note that strongly asymmetric elements always exist by [DGO11, Lemma 6.18].

Example 3. Let S be a closed genus 2 surface, and let $\tilde{S} \rightarrow S$ be a degree 2 cover, so \tilde{S} is a closed genus 3 surface. Let G be the mapping class group of \tilde{S} , which has trivial maximal finite normal subgroup, and let $T \cong \mathbb{Z}/2\mathbb{Z}$ be the subgroup of G consisting of covering transformations. Any pseudo-Anosov map $g: S \rightarrow S$ has a power which lifts to a map $\tilde{g}: \tilde{S} \rightarrow \tilde{S}$, which commutes with T , so $\langle \tilde{g} \rangle \times T < E(\tilde{g})$, and so \tilde{g} is not weakly asymmetric.

We now describe the particular model of random subgroups which we shall consider. A *random subgroup* of G with k generators is a subgroup whose generators are chosen to be independent random walks of length n_i on G . We will require the following restrictions on the probability distributions μ_i generating the random walks. We say a probability distribution μ on G is non-elementary if the group generated by its support is non-elementary.

Definition 4. Let G act acylindrically hyperbolically on X . We say that the probability distribution μ on G is $(G \curvearrowright X)$ -*admissible* if the support of μ generates a non-elementary subgroup of G containing a weakly asymmetric element, and furthermore, the support of μ has bounded image in X .

The set of admissible measures depends on the action of G on X , though we shall suppress this from our notation and just write *admissible* for $(G \curvearrowright X)$ -admissible. We shall write $\tilde{\mu}$ for the reflected probability distribution $\tilde{\mu}(g) = \mu(g^{-1})$, and $\tilde{\mu}$ is admissible if and only if μ is admissible.

We may now give a precise definition of our model for random subgroups. Let μ_1, \dots, μ_k be a finite collection of admissible probability distributions on G . We shall write $H(\mu_1, \dots, \mu_k, n_1, \dots, n_k)$ to denote the subgroup generated by $\langle w_{1,n_1}, \dots, w_{k,n_k} \rangle$, where each w_{i,n_i} is a group element arising from a random walk on G of length n_i generated by μ_i . To simplify notation we shall often just write $H(\mu_i, n_i)$, or just H , for $H(\mu_1, \dots, \mu_k, n_1, \dots, n_k)$. We may now state our main result.

Theorem 5. *Let G be a countable group acting acylindrically hyperbolically on the separable space X , and let $E(G)$ be the maximal finite normal subgroup of G . Let $H(\mu_1, \dots, \mu_k, n_1, \dots, n_k)$ be a random subgroup of G , where the μ_i are admissible probability distributions on G . Then the probability that each of the following three events occurs tends to one as $\min n_i$*

tends to infinity.

1. All of the w_{i,n_i} are hyperbolic and weakly asymmetric.
2. The subgroup H is freely generated by the $\{w_{i,n_i}\}$ and quasi-isometrically embedded in X , and so in particular $HE(G)$ is a semidirect product $H \ltimes E(G)$.
3. The subgroup $H \ltimes E(G)$ is geometrically separated in X .

In general the semidirect product $H \ltimes E(G)$ need not be the product $H \times E(G)$ for random subgroups H , as shown below.

Example 6. Let G be a group acting acylindrically hyperbolically on X with trivial maximal finite normal subgroup $E(G)$, which admits a split extension

$$1 \rightarrow F \rightarrow G^+ \rightarrow G \rightarrow 1,$$

which is not a product, for some finite group F . Such a split extension is determined by a homomorphism $\phi: G \rightarrow \text{Aut}(F)$, where $\text{Aut}(F)$ is the automorphism group of F . The maximal finite normal subgroup $E(G)$ is equal to F . A random walk on G^+ pushes forward to a random walk on G , and then to a random walk on $\phi(G) < \text{Aut}(F)$. As $\phi(G)$ is finite, the random walk is asymptotically uniformly distributed. A hyperbolic group element g has $E(g) = \langle g \rangle \times F$ if and only if the image of g in $\phi(G)$ is trivial, which happens with asymptotic probability $1/|\phi(G)|$.

In the next section, Section 2.1, we recall the definition of a hyperbolically embedded subgroup, and show how Theorem 1 follows from Theorem 5.

2.1 Hyperbolically embedded subgroups

Osin [Osi16] showed that if a group is acylindrically hyperbolic, then there is a (not necessarily finite) generating set Y , such that the Cayley graph of G with respect to Y , which we shall denote $\text{Cay}(G, Y)$, is hyperbolic, and the action of G on $\text{Cay}(G, Y)$ is acylindrical and non-elementary. In general, there are many choices of Y giving non-quasi-isometric acylindrically hyperbolic actions, for which different collections of subgroups will be hyperbolically embedded, but for the remainder of this section we shall assume we have chosen some fixed Y .

Let H be a subgroup of G ; we will write $\text{Cay}(G, Y \sqcup H)$ for the Cayley graph of G with respect to the disjoint union of Y and H (so it might have double edges). The Cayley graph $\text{Cay}(H, H)$ is a complete subgraph of $\text{Cay}(G, Y \sqcup H)$. We say a path p in $\text{Cay}(G, Y \sqcup H)$ is *admissible* if it does not contain edges of $\text{Cay}(H, H)$, though it may contain edges of non-trivial cosets of H , and may pass through vertices of H . We define a

restriction metric \hat{d}_H on H be setting $\hat{d}_H(h_1, h_2)$ to be the minimal length of any admissible path in $\text{Cay}(G, Y \sqcup H)$ connecting h_1 and h_2 . If no such path exists we set $\hat{d}_H(h_1, h_2) = \infty$.

We say a finitely generated subgroup H of a finitely generated acylindrically hyperbolic group G is *hyperbolically embedded* in G with respect to a generating set $Y \subset G$ if the Cayley graph $\text{Cay}(G, Y \sqcup H)$ is hyperbolic, and \hat{d}_H is proper. We shall denote this by $H \hookrightarrow_h (G, Y)$.

We shall use the following sufficient conditions for a subgroup to be hyperbolically embedded, due to Hull [Hul13, Theorem 3.16] and Antolin, Minasyan and Sisto [AMS16, Theorem 3.9, Corollary 3.10] (both refinements of Dahmani, Guirardel and Osin [DGO11, Theorem 4.42]), which we now describe.

Theorem 7. [Hul13, AMS16] *Suppose that G acts acylindrically hyperbolically on X . Let H be a finitely generated subgroup of G , which is quasi-isometrically embedded and geometrically separated in X . Then H is hyperbolically embedded in G . Moreover, if $X = \text{Cay}(G, Y)$ for some $Y \subseteq G$, then $H \hookrightarrow_h (G, Y)$.*

Theorem 1 now follows immediately from Theorem 5 and Theorem 7, choosing X to be $\text{Cay}(G, Y)$. In fact, we have the following refinement, which we record for future reference:

Theorem 8. *Let the finitely generated group G act acylindrically hyperbolically on its Cayley graph $\text{Cay}(G, Y)$, and let $E(G)$ be the maximal finite normal subgroup of G . Let $H(\mu_1, \dots, \mu_k, n_1, \dots, n_k)$ be a random subgroup of G , where the μ_i are admissible probability distributions on G . Then the probability that each of the following events occurs tends to one as $\min n_i$ tends to infinity.*

1. *The subgroup H is freely generated by the $\{w_{i, n_i}\}$, and in particular $HE(G)$ is a semidirect product $H \rtimes E(G)$.*
2. *$H \rtimes E(G) \hookrightarrow_h (G, Y)$.*

2.2 Outline

We conclude this section with a brief outline of the rest of the paper, using the notation of Theorem 5. In the final part of this section, Section 2.3, we recall some basic concepts and define some notation. In Section 3 we review some estimates for the behaviour of random walks. In Section 3.1 we review some exponential decay estimates that we will use, including the fact that a random walk makes linear progress in X , with the probability of a linearly large deviation tending to zero exponentially quickly, an estimate for the Gromov product of the initial and final point of a

random walk, based at an intermediate point, and the property that the hitting measure of a shadow set in X decays exponentially in its distance from the basepoint.

In Section 3.2 we review some matching estimates, which we now describe. We say two geodesics α and β in X have an (A, B) -match, if there is a subgeodesic of one of length A which has a translate by some element of G which B -fellow travels the other one; we say that a single geodesic γ has an (A, B) -match if there is a subgeodesic of γ of length A which B -fellow travels a disjoint subgeodesic. If the constant B can be chosen to only depend on δ , the constant of hyperbolicity, then we may refer to an (A, B) -match as a match of length A . Let γ_n be a geodesic in X from x_0 to $w_n x_0$. For any geodesic η , the probability that η has a match of length $|\eta|$ with γ_n decays exponentially in $|\eta|$, and this can be used to show that the probability that γ_n has a match of linear length (with itself) tends to zero as n tends to infinity. We will also use the facts that if γ_ω is the bi-infinite geodesic determined by a bi-infinite random walk, and α_n is an axis for w_n , assuming w_n is hyperbolic, then the probability that γ_n, γ_ω and α_n have matches of a size which is linear in n , tends to 1 as n tends to infinity. Finally, we also use the fact that for any group element g in the support of μ with axis γ_g , ergodicity implies that the bi-infinite geodesic γ_ω has infinitely many matches with γ_g of arbitrarily large length.

In Section 4 we recall some standard results about free subgroups of a group G acting by isometries on a Gromov hyperbolic space X . In particular, as shown by, e.g., Taylor and Tiozzo [TT16], if a subgroup H has a symmetric generating set $A = \{a_1, a_1^{-1}, \dots, a_k, a_k^{-1}\}$, for which the distances $d_X(x_0, ax_0)$ are large, for all a in A , and the Gromov products $(ax_0 \cdot bx_0)_{x_0}$ are small, for all distinct a and b in A , then $\{a_1, \dots, a_k\}$ freely generates a free group H , which is quasi-isometrically embedded in X . We show that furthermore, if Γ_H is a rescaled copy of the Cayley graph, in which an edge corresponding to $a \in A$ has length $d_X(x_0, ax_0)$, then Γ_H is quasi-isometrically embedded in H , with quasi-isometry constants depending only on δ and the size of the largest Gromov product $(ax_0 \cdot bx_0)_{x_0}$, and not on the lengths of the geodesics $[x_0, ax_0]$, for $a \in A$.

In Section 5 we prove a version of Theorem 5 in the case that the group has a single generator, i.e. $k = 1$, which is equivalent to showing that the probability that w_n is hyperbolic and weakly asymmetric tends to one with asymptotic probability one. In Section 5.1 we define coarse analogues of the following properties of group elements: being primitive and being asymmetric, and we show that these conditions are sufficient to show that a group element is weakly asymmetric, as long as it is not conjugate to its inverse. Then in Section 5.2, we use the matching estimates to show

that the coarse analogues hold with asymptotic probability one, as does the property that w_n is not conjugate to its inverse.

A key step is to use the fact that the support of μ contains a weakly asymmetric element, g say, with axis α_g . A result of Bestvina and Fujiwara [BF02] says that if a group element h coarsely stabilizes a sufficiently long segment of α_g , then in fact h lies in $E(g)$. Ergodicity implies that the bi-infinite geodesic γ_ω fellow travels infinitely often with long segments of translates of α_g , and the matching estimates then imply that the axis α_n for w_n also fellow travels with long segments of translates of α_g , with asymptotic probability one. Therefore an element $h \in E(g)$ which coarsely fixes α_n pointwise must also stabilize disjoint translates of long segments of α_g , $h_1\alpha_g$ and $h_2\alpha_g$ say. This implies that h lies in $(h_1\langle g \rangle h_1^{-1} \times (E(g))) \cap (h_2\langle g \rangle h_2^{-1} \times E(g)) = E(g)$, and so w_n is weakly asymmetric.

Finally, in Section 6, we extend this result to finitely generated random subgroups. Let w_{i,n_i} be the generators of H , and let γ_{i,n_i} be a geodesic from x_0 to $w_{i,n_i}x_0$. The random walk corresponding to each generator makes linear progress, and pairs of independent random walks satisfy an exponential decay estimate for the size of their Gromov products based at the basepoint x_0 , so this shows that H is asymptotically freely generated by the locations of the sample paths w_{i,n_i} , and is quasi-isometrically embedded in X . If H is not geometrically separated, then there is an arbitrarily large intersection of $N_R(gH)$ and $N_R(H)$, which implies that there is a pair of long geodesics γ and γ' with endpoints in H such that $g\gamma'$ fellow travels with γ , for $g \in G \setminus (H \times E(G))$. The probability that γ_{i,n_i} matches any combination of shorter generators tends to zero, so for some i , the group element g takes some translate $h_1\gamma_{i,n_i}$ say, to another translate $h_2\gamma_{i,n_i}$. This implies that $h_2^{-1}gh_1$ coarsely stabilizes γ_{i,n_i} , and so g lies in $h_2(\langle w_{i,n_i} \rangle \times E(G))h_1 \subset H \times E(G)$, by the fact that each individual random walk gives weakly asymmetric elements with asymptotic probability one. This contradicts our initial assumption that g did not lie in $H \times E(G)$.

2.3 Notation and standing assumptions

Throughout the paper we fix a group G acting acylindrically hyperbolically on a separable hyperbolic space X . We will always assume that the hyperbolic space X is geodesic, but it need not be locally compact. We denote the distance in X by d_X , and δ will refer to the constant of hyperbolicity for the Gromov hyperbolic space X . We will write $O(\delta)$ to refer to a constant which only depends on δ , through not necessarily linearly. We shall write $|\gamma|$ for the length of a path γ . If γ is a geodesic, then $|\gamma|$ is

equal to the distance between its endpoints. Geodesics will always have unit speed parameterizations, and $\gamma(t)$ will denote a point on γ distance t from its initial point, and we will write $[\gamma(t), \gamma(t')]$ for the subgeodesic of γ from $\gamma(t)$ to $\gamma(t')$.

In all statements about a single random walk on G , we will assume that the random walk is generated by an admissible probability measure μ and denote the position of the walk at time n by w_n , while the corresponding notations for multiple random walks will be μ_i for the admissible measures and w_{i,n_i} for the locations of the random walks.

If we say that a constant A depends on an admissible probability measure μ , then as the set of admissible measures depends on the action of G on X , we allow that A may also depend on the action, and also on the constant of hyperbolicity δ , and the acylindricity functions $R(K)$ and $N(K)$. If we say that a constant A depends on the collection of probability distributions μ_1, \dots, μ_k corresponding to a random subgroup H , this includes the possibility that the constant may depend on the number k of probability distributions. We will occasionally recall some of these assumptions and notations.

3 Estimates for random walks

3.1 Exponential decay

Let μ be an admissible probability distribution on G . We will make use of the following exponential decay estimates, as shown by Maher and Tiozzo [MT14] and Mathieu and Sisto [MS14]. We denote the Gromov product by $(x \cdot y)_w$, which by definition is

$$(x \cdot y)_w = \frac{1}{2}(d_X(w, x) + d_X(w, y) - d_X(x, y)).$$

Furthermore, as the distance the sample path has moved in X is subadditive, the limit

$$L = \lim_{n \rightarrow \infty} \frac{1}{n} d_X(x_0, w_n x_0)$$

exists almost surely, and L is the same for almost all sample paths, by ergodicity. If μ is admissible then L is positive, and we say that the random walk has positive drift, or makes linear progress.

Given $x_0, x \in X$ and $R > 0$, the *shadow* $S_{x_0}(x, R)$ is defined to be

$$S_{x_0}(x, R) = \{y \in X : (x \cdot y)_{x_0} \geq d_X(x_0, x) - R\}.$$

Proposition 9. *Let G be a countable group which acts acylindrically hyperbolically on a separable space X with basepoint x_0 , and let μ be an admissible probability distribution on G . Then the following exponential decay estimates hold:*

9.1 Positive drift in X with exponential decay.

There is a positive drift constant $L > 0$ such that for any $\varepsilon > 0$ there are constants $K > 0$ and $c < 1$, depending on μ and x_0 , such that

$$\mathbb{P}((1 - \varepsilon)Ln \leq d_X(x_0, w_n x_0) \leq (1 + \varepsilon)Ln) \geq 1 - Kc^n, \quad (1)$$

for all n .

9.2 Exponential decay for Gromov products in X .

There are constants $K > 0$ and $c < 1$, depending on μ and x_0 , such that for all i, n and r ,

$$\mathbb{P}((x_0 \cdot w_n x_0)_{w_i x_0} \geq r) \leq Kc^r \quad (2)$$

9.3 Exponential decay for shadows in X .

There is a constant $R_0 > 0$, which only depends on the action of G on X , and constants $K > 0$ and $c < 1$, which depend on μ and x_0 , such that for all g and $R \geq R_0$,

$$\mathbb{P}(w_n \in S_{x_0}(gx_0, R)) \leq Kc^{d_X(x_0, gx_0) - R}. \quad (3)$$

3.2 Matching

A *match* for a pair of geodesics in X , is a subsegment of one geodesic, which may be translated by an element of G to fellow travel with a subsegment of the other one. We now give a precise definition.

We say that two geodesics γ and γ' in X have an (A, B) -*match* if there are disjoint subgeodesics $\alpha \subset \gamma$ and $\alpha' \subset \gamma'$ of length at least A , and a group element $g \in G$, such that the Hausdorff distance between $g\alpha$ and α' is at most B . We may choose γ and γ' to be the same geodesic, or overlapping geodesics. If γ and γ' are the same geodesic, then we will just say that γ has an (A, B) -match.

Given w_n , a random walk of length n on G , we shall write γ_n for a geodesic in X from x_0 to $w_n x_0$. As sample paths converge to the Gromov boundary ∂X almost surely [MT14], a bi-infinite sample path $\{w_n x_0\}_{n \in \mathbb{Z}}$ determines a bi-infinite geodesic in X almost surely, which we shall denote γ_ω .

In an arbitrary non-locally compact Gromov hyperbolic space, pairs of points in the boundary need not be connected by bi-infinite geodesics, however, they are always connected by $(1, O(\delta))$ -quasigeodesics. With a slight abuse of language, we will call any bi-infinite $(1, O(\delta))$ -quasigeodesic connecting the limit points of g an *axis* for the hyperbolic element g .

Proposition 10. *Let G be a countable group which acts acylindrically hyperbolically on the separable space X , and let μ be an admissible probability distribution on G . Then there is a constant K_0 , depending only on δ , such that for any $K \geq K_0$, the following matching estimates hold.*

- 10.1 *There are constants B and c , depending on μ and K , such that for any geodesic segment η and any constant t , the probability that a translate of η is contained in a K -neighbourhood of $[\gamma_n(t), \gamma_n(t+|\eta|)]$ is at most $Bc^{|\eta|}$.*
- 10.2 *For any $\varepsilon > 0$ the probability that γ_n has an $(\varepsilon|\gamma_n|, K)$ -match tends to zero as n tends to infinity.*
- 10.3 *For any $\varepsilon > 0$, the probability that the γ_n contains a subsegment of length at least $(1-\varepsilon)|\gamma_n|$ which is contained in a K -neighbourhood of γ_ω tends to one as n tends to infinity. In particular, the probability that γ_n and γ_ω have an $((1-\varepsilon)|\gamma_n|, K)$ -match tends to one as n tends to infinity.*
- 10.4 *Let g be a hyperbolic isometry with axis α_g which lies in the support of μ . Then for any constants $0 < \varepsilon < \frac{1}{3}$ and $L \geq 0$, the probability that γ_n^- and α_g have an (L, K) -match tends to one as n tends to infinity, where γ_n^- is the subgeodesic of γ_n obtained by removing $\varepsilon|\gamma_n|$ -neighbourhoods of its endpoints.*
- 10.5 *For any $\varepsilon > 0$, the probability that w_n is hyperbolic with axis α_n , and γ_n and α_n have a $((1-\varepsilon)|\gamma_n|, K)$ -match tends to one as n tends to infinity.*

Propositions 10.1, 10.2 and 10.3 are shown by Calegari and Maher [CM15]. Proposition 10.1 is not stated explicitly, but follows directly from the proof of [CM15, Lemma 5.26].

Proposition 10.5 is shown for μ with finite support by Dahmani and Horbez [DH15, Proposition 1.5]. However, they only need finite support to ensure linear progress with exponential decay, and exponential decay for shadows, and so their argument also works for μ with bounded support in X .

Finally, a version of Proposition 10.4 is shown for the mapping class group acting on Teichmüller space, for μ with finite support, by Gadre and Maher [GM16], and independently by Baik, Gekhtman and Hamenstädt [BGH16]. A significantly simpler version of these arguments works in the setting of acylindrically hyperbolic groups, but we present the details below for the convenience of the reader. As a side remark, we note that it can be shown that, in fact, the largest match of γ_n and α_g has logarithmic size in n [ST16].

Proof (of Proposition 10.4). Let g be a hyperbolic element which lies in the support of μ , and let α_g be an axis for g . Let γ_ω be the bi-infinite geodesic determined by a bi-infinite random walk generated by μ . We shall write ν for the harmonic measure on ∂X , and $\check{\nu}$ for the reflected harmonic measure, i.e the harmonic measure arising from the random walk generated by the probability distribution $\check{\mu}(g) = \mu(g^{-1})$.

By assumption, the group element g lies in the support of μ , and so the group element g^{-1} lies in the support of $\check{\mu}$. Given a constant $L > 0$, there is an m sufficiently large such that any geodesic from $S_{x_0}(g^m x_0, R_0)$ to $S_{x_0}(g^{-m} x_0, R_0)$ has a subsegment of length L which $K = O(\delta)$ -fellow travels with α_g . The following result of Maher and Tiozzo [MT14] guarantees that the harmonic measures of these shadow sets are positive.

Proposition 11. [MT14, Proposition 5.4] *Let G be a countable group acting acylindrically hyperbolically on a separable space X , and let μ be a non-elementary probability distribution on G . Then there is a number R_0 such that for any group element g in the semigroup generated by the support of μ , the closure of the shadow $S_{x_0}(gx_0, R_0)$ has positive hitting measure for the random walk determined by μ .*

Therefore $\nu(S_{x_0}(g^m x_0, R_0)) > 0$ and $\check{\nu}(S_{x_0}(g^{-m} x_0, R_0)) > 0$, and so there is a positive probability p say that γ_ω has a subsegment of length at least L which lies in a K -neighbourhood of γ_g . Ergodicity now implies that the proportion of times in $\{\lfloor \frac{n}{3} \rfloor, \dots, \lfloor \frac{2n}{3} \rfloor\}$ for which γ_ω has a subsegment of length at least L which lies in a K -neighbourhood of $w_m \gamma_g$ tends to p as n tends to infinity, for almost all sample paths ω . Proposition 10.3 then implies that the probability that γ_n has an (L, K) -match with γ_g tends to one. \square

4 Schottky groups

In this section we collect together some standard results about free subgroups of a group G acting by isometries on a hyperbolic space X , see for example Bridson and Haefliger [BH99] for a thorough discussion. For completeness, we present a mild generalization of an argument due to Taylor and Tiozzo [TT16], and show that one may rescale the Cayley graph Γ of a Schottky group so that the quasi-isometric embedding constants of Γ into X depend only on δ , the constant of hyperbolicity for X , and the size of the Gromov products between the generators.

A relation $g = g_1 g_2 \dots g_n$ between elements of G may be thought of as a recipe for assembling a path from x_0 to gx_0 as a concatenation of translates of paths from x_0 to $g_i x_0$. The following proposition gives an

estimate for the distance of the endpoints of the total path in terms of the lengths of the shorter segments, and the Gromov products between adjacent segments.

Let η be a path which is a concatenation of k geodesic segments $\{\eta_i\}_{i=1}^k$, and label the endpoints of η_i as x_{i-1} and x_i , such that the common endpoint of η_i and η_{i+1} is labelled x_i . For $2 \leq i \leq k$, let p_i be the nearest point projection of x_{i-2} to η_i , and for $1 \leq i \leq k-1$, let q_i be the nearest point projection of x_{i+1} to η_i . We define $p_1 = x_0$ and $q_k = x_{k+1}$. We will call the subsegment $[p_i, q_i] \subset \eta_i$ the *persistent subgeodesic* of η_i . This is illustrated below in Figure 1.

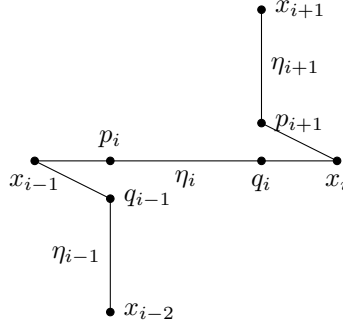


Figure 1: A concatenation of geodesic segments.

The length of the persistent subgeodesic may be estimated in terms of Gromov products.

Proposition 12. *There is a constant C , which only depends on δ such that if η is a concatenation of geodesic segments η_i , with persistent subgeodesics $[p_i, q_i]$, then*

$$d_X(p_i, q_i) \leq d_X(x_{i-1}, x_i) - (x_{i-2} \cdot x_i)_{x_{i-1}} - (x_{i-1} \cdot x_{i+1})_{x_i} + C,$$

and

$$d_X(p_i, q_i) \geq d_X(x_{i-1}, x_i) - (x_{i-2} \cdot x_i)_{x_{i-1}} - (x_{i-1} \cdot x_{i+1})_{x_i} - C. \quad (4)$$

We omit the proof of Proposition 12, which is a straight forward application of thin triangles and the definition of the Gromov product.

We now show that if each persistent subsegment is sufficiently long, then the distance between x_0 and x_k is equal to the sum of the lengths of the persistent subsegments, up to an additive error proportional to the number of geodesic segments.

Proposition 13. *There exists a constant $C > 0$, which depends only on δ , such that if η is a concatenation of geodesic segments η_i for $1 \leq i \leq k$, with persistent subgeodesics $[p_i, q_i]$ with*

$$d_X(p_i, q_i) \geq C, \quad (5)$$

for all $1 \leq i \leq k$, then

$$\sum_{i=1}^k d_X(p_i, q_i) - 2Ck \leq d_X(x_0, x_k) \leq \sum_{i=1}^k d_X(p_i, q_i) + 2Ck. \quad (6)$$

Furthermore, any geodesic from x_0 to x_k passes within distance C of both p_i and q_i .

Proof. For any three points x, y and z , determining a triangle in X , there is a point m , known as the *center* of triangle, such that m is distance at most δ from each of the three sides of the triangle. Furthermore, there is a C_1 , which only depends on δ , such that if p is a closest point on $[y, z]$ to x , then $d_X(p, m) \leq C_1$. This implies that $d_X(q_i, p_{i+1}) \leq 2C_1$, using the triangle with vertices x_{i-1}, x_i and x_{i+1} . The upper bound

$$d_X(x_0, x_k) \leq d_X(q_i, p_{i+1}) + 2C_1k$$

then follows from the triangle inequality.

There are constants C_2 and C_3 , which only depend on δ , such that for any point y in X , whose nearest point projection to η_{i-1} is distance at least C_2 away from η_i , the nearest point projection of y to η_i is distance at most C_3 from p_i . As this also holds for η_{i-1} , the nearest point projection of x_{i-3} to η_{i-1} is within distance C_3 of p_{i-1} , and so the nearest point projection of x_{i-3} to η_i is within distance C_3 of p_i . By induction, the nearest point projection of x_0 to η_i is within distance C_3 of p_i , and similarly, the nearest point projection of x_k to η_i is within distance C_3 of q_i .

There are constants C_4 and C_5 , depending only on δ , such that if two points x and y in X have nearest point projections p and q onto a geodesic α , and $d_X(p, q) \geq C_4$, then any geodesic from x to y passes within distance C_5 of both p and q .

In particular, there exists C_6 depending only on δ so that if γ is a geodesic from x_0 to x_k , then for each i there is a subsegment of γ of length at least $d_X(p_i, q_i) - C_6$ which is contained in a $C_5 + 4\delta$ -neighbourhood of the persistent subsegment $[p_i, q_i]$, and is disjoint from $C_5 + 4\delta$ -neighbourhoods of the other persistent subsegments $[p_j, q_j]$ for $i \neq j$. Therefore

$$d_X(x_0, x_k) \geq \sum_{i=1}^k (d_X(p_i, q_i) - C_6),$$

giving the required lower bound. \square

We now use Proposition 13 to give a lower bound on the translation length of group elements.

Proposition 14. *There exists a constant $C > 0$, which depends only on δ , such that if g is an isometry of a hyperbolic space X with basepoint x_0 , which is a product of isometries $g = g_1 g_2 \dots g_n$, where the g_i satisfy the following collection of inequalities*

$$d_X(x_0, g_i x_0) \geq (g_{i-1}^{-1} x_0 \cdot g_i x_0)_{x_0} + (g_i^{-1} x_0 \cdot g_{i+1} x_0)_{x_0} + C, \quad (7)$$

where $g_{n+1} = g_1$ and $g_0 = g_n$, then the translation length of g is at least

$$\tau(g) \geq \sum_{i=1}^n (d_X(x_0, g_i x_0) - (g_{i-1}^{-1} x_0 \cdot g_i x_0)_{x_0} - (g_i^{-1} x_0 \cdot g_{i+1} x_0)_{x_0} + C), \quad (8)$$

and furthermore, any geodesic from x_0 to $g x_0$, and any axis γ for g passes within distance $(g_{i-1}^{-1} x_0 \cdot g_i x_0)_{x_0} + (g_i^{-1} x_0 \cdot g_{i+1} x_0)_{x_0} + C$ of each $g_1 \dots g_i x_0$.

Proof. We first define a sequence of points $\{x_i\}_{i=0}^n$, and a sequence of geodesic segments $\{\eta_i\}_{i=1}^n$, following the index conventions of Proposition 12. Let x_0 be the basepoint of X , and for $1 \leq i \leq n$ let $x_i = g_1 \dots g_i x_0$. For $1 \leq i \leq n$ let η_i be a geodesic from x_{i-1} to x_i , and let η be the path formed from the concatenation of the geodesic segments η_i .

We may now consider the bi-infinite sequences obtained from all g -translates of the points x_i and the geodesics η_i , labelled such that $x_{jn+i} = g^j x_i$ and $\eta_{jn+i} = g^j \eta_i$, for $j \in \mathbb{Z}$ and $1 \leq i \leq n$. The terminal point x_n of η_n is equal to $g_1 \dots g_n x_0 = g x_0$, which is the same as the initial point of $\eta_{n+1} = g \eta_1 = g x_0$, so the concatenation of the geodesics η_i is a bi-infinite g -equivariant path in X , which we shall denote η .

If we choose $C \geq 3C_1$, where C_1 is the constant from Proposition 13 then the assumption (7), together with the estimate for persistent length in terms of Gromov products (4), implies that any subpath $\{\eta_i\}_{i=a}^b$ of η satisfies the hypothesis of Proposition 13, and so the conclusion of Proposition 13 implies that $d_X(x_{a-1}, x_b) \geq C_1(b-a)$. In particular, this implies that the translation length $\tau(g)$, which by definition is equal to

$$\tau(g) = \lim_{m \rightarrow \infty} \frac{1}{m} d_X(x_0, g^m x_0),$$

is given by

$$\tau(g) = \lim_{m \rightarrow \infty} \frac{1}{m} d_X(x_0, x_{mn}) \geq C_1 n > 0.$$

Therefore the translation length $\tau(g)$ is positive, and so g is hyperbolic, and η is a quasi-axis for g . The estimate for translation length (8) then follows by combining (4) and (6), and the statements about the distance from x_i to any geodesic γ from x_a to x_b , for $a \leq i \leq b$, and the distance from x_i to any axis for g follow from thin triangles and the definition of the Gromov product, for $C = 3C_1 + O(\delta)$. \square

We now give conditions on the generators of a subgroup which ensure that the generators freely generate a subgroup which is quasi-isometrically embedded in X .

Given a symmetric generating set $A = \{a_1, a_1^{-1}, \dots, a_k, a_k^{-1}\}$ generating a subgroup H of G , let $F_{\overline{A}}$ be the free group generated by $\overline{A} = \{a_1, \dots, a_k\}$, and let Γ_H be a rescaled copy of the Cayley graph for $F_{\overline{A}}$, with respect to the generating set \overline{A} , where an edge in Γ_H corresponding to a generator a_i has length equal to $d_X(x_0, a_i x_0)$. We shall refer to Γ_H as the *rescaled Cayley graph* for $F_{\overline{A}}$, which is quasi-isometric to the standard unscaled Cayley graph in which every edge has length one. The map from Γ_H to X which sends a vertex h to hx_0 , and an edge from h to h' to a geodesic from hx_0 to $h'x_0$ is continuous, can be made H -equivariant, and is an isometric embedding on each edge. The conditions we give below will in fact show that Γ_H is quasi-isometrically embedded in X , with quasi-isometry constants independent of the lengths of the edges.

Proposition 15. *There is a constant K_0 , which only depends on δ , such that for any $K \geq K_0$, if H is a subgroup generated by the symmetric generating set $A = \{a_1, a_1^{-1}, \dots, a_k, a_k^{-1}\}$, satisfying the following conditions,*

$$\left. \begin{array}{l} d_X(x_0, ax_0) \geq 6K \text{ for all } a \in A \\ (ax_0 \cdot bx_0)_{x_0} \leq K \text{ for all } a \neq b \text{ in } A \end{array} \right\} \quad (9)$$

then H is isomorphic to the free group F_k , freely generated by the generating set $\overline{A} = \{a_1, \dots, a_k\}$, and furthermore, the subgroup H is quasi-isometrically embedded in X , and the rescaled Cayley graph Γ_H is $(6, O(\delta, K))$ -quasi-isometrically embedded in X .

Proof. We shall choose $K_0 > 2C$, where C is the constant from Proposition 14. Let $g = g_1 \dots g_n$ be a reduced word in the generating set A . The g_i satisfy the Gromov product inequalities from (7). Proposition 14 then implies that $\tau(g) \geq Cn$, so in particular all reduced words are non trivial, so \overline{A} freely generates a free group.

We now show that Γ_H is quasi-isometrically embedded in X , for quasi-isometry constants that are independent of the lengths of the g_i . The translation length $\tau(g)$ is a lower bound for $d_X(x_0, gx_0)$, and as $g_1 \dots g_n$ is a reduced word

$$d_{\Gamma_H}(x_0, gx_0) = \sum_{i=1}^n d_X(x_0, g_i x_0).$$

Therefore conclusion (8) of Proposition 14 implies the left hand bound below

$$d_{\Gamma_H}(x_0, gx_0) - 5Kk \leq d_X(x_0, gx_0) \leq d_{\Gamma_H}(x_0, gx_0),$$

where $K \geq K_0$, for the choice of K_0 given above. The right hand bound follows immediately from the triangle inequality. As each geodesic segment of Γ_H has length at least $6K$, this implies

$$\frac{1}{6}d_{\Gamma_H}(x_0, gx_0) \leq d_X(x_0, gx_0) \leq d_{\Gamma_H}(x_0, gx_0).$$

Finally, using thin triangles, we may extend this estimate to all points x and y in Γ_H to obtain

$$\frac{1}{6}d_{\Gamma_H}(x, y) - 2K + O(\delta) \leq d_X(x_0, gx_0) \leq d_{\Gamma_H}(x_0, gx_0) + 2K + O(\delta).$$

as required. \square

5 Special case: one generator

The probability that w_n is hyperbolic tends to one, so in particular, if $X = \text{Cay}(G, Y)$, then the probability that $E(w_n)$ is hyperbolically embedded in (G, Y) tends to one. In this section we show that the probability that w_n is weakly asymmetric tends to one, i.e. the probability that $E(w_n) = \langle w_n \rangle \rtimes E(G)$ tends to one, and this is precisely the special case of Theorem 5 when $k = 1$.

Proposition 16. *Let G be a countable group acting acylindrically hyperbolically on the separable space X , and let μ be an admissible probability distribution on G . Then the probability that w_n is hyperbolic and weakly asymmetric tends to one as n tends to infinity.*

We start in Section 5.1 by giving some geometric conditions which are sufficient to show that a group element is weakly asymmetric. In Section 5.2 we show that the probability that these conditions are satisfied by a random element w_n tends to one as n tends to infinity.

5.1 Asymmetric elements

Let g be a hyperbolic isometry. Recall that a group element $g \in G$ is *primitive* if there is no element $h \in G$ such that $h^n = g$ for $n > 1$. We now define a notion of coarse primitivity for group elements.

Definition 17. Let γ be an axis for g , let p_i be the projection of $g^i x_0$ to γ , and set $P = \bigcup_{i \in \mathbb{Z}} p_i$. We say that g is *K -primitive* if any element $h \in E(g)$ K -stabilizes P , i.e. the Hausdorff distance $d_{\text{Haus}}(P, hP) \leq K$.

If g is K -primitive, then g is primitive, for $K = O(\delta)$ sufficiently large, and if the translation distance $\tau(g)$ satisfies $\tau(g) > K + O(\delta)$.

Recall that for a hyperbolic element g , $\Lambda(g) = \{\lambda_+(g), \lambda_-(g)\}$ is the set consisting of the pair of attracting and repelling fixed points for g in ∂X ,

and $E(g) = \text{stab}(\Lambda(g))$. We shall write $E^+(g)$ for the subgroup of $E(g)$ which preserves $\Lambda(g)$ pointwise, i.e. $E^+(g) = \text{stab}(\lambda_+(g)) \cap \text{stab}(\lambda_-(g))$. This subgroup has index at most 2 in $E(g)$.

Definition 18. We say a hyperbolic isometry g is *reversible* if there is an element in $E(g)$ which switches the fixed points of g , i.e. $E^+(g) \subsetneq E(g)$. Otherwise g is *irreversible* and $E^+(g) = E(g)$.

We say that the K -stabilizer of a geodesic $\gamma = [p, q]$, consists of all group elements g such that if $d_X(p, gp) \leq K$ and $d_X(q, hq) \leq K$.

Definition 19. Let G be a countable group acting acylindrically hyperbolically on a separable space X . We say that a group element g is *K-asymmetric* if g is hyperbolic with axis α_g , and if p is a closest point on α_g to the basepoint x_0 , then the K -stabilizer for the geodesic $[p, gp]$ is equal to $E(G)$.

We first show that every non-elementary subgroup H of G containing a weakly asymmetric element, also contains a K -asymmetric element.

Proposition 20. *Let G be a countable group acting acylindrically hyperbolically on a separable space X , and let H be a non-elementary subgroup of G , which contains a weakly asymmetric element. Then for any constant $K \geq 0$, the subgroup H contains a K -asymmetric element g .*

We will use the following lemma, which follows from work of Bestvina and Fujiwara.

Lemma 21. [BF02, Proposition 6] *Let g be a hyperbolic isometry with axis α_g . Then for any number $K \geq 0$ there is a D , depending on g, δ and K , such that if h K -coarsely stabilizes a segment of α_g of length at least D , then h lies in $E(g)$.*

Proof (of Proposition 20). Let h be a weakly asymmetric element in H , with axis γ_h . As H is non-elementary, and $E(h)$ is virtually cyclic, there is a hyperbolic element f in H which does not lie in $E(h)$. In particular, h and f are independent, i.e. their fixed point sets in ∂X are disjoint. Consider the group element $g = h^a f^b h^a$. For all a and b sufficiently large, the translation lengths of h^a and f^b are much larger than twice any of the Gromov products between distinct elements of $\{h^{\pm a}, f^{\pm b}\}$, so we may apply Proposition 14, which in particular implies that g is hyperbolic. Furthermore, for any constant $D > 0$, there is an a sufficiently large such that the axis γ_g of g has a subsegment γ_1 of length at least D which is contained in an $O(\delta)$ -neighbourhood of γ_h , and a disjoint subsegment γ_2 of length at least D which is contained in an $O(\delta)$ -neighbourhood of $h^a f^b \gamma_h$. We shall choose an a sufficiently large such that this holds for $D > D_h + O(K, \delta)$, where D_h is the constant from Lemma 21 applied to the hyperbolic element h with constant $K + O(\delta)$. Finally, we may choose

a to be much larger than b , so that D is at least three times as large as the distance between γ_1 and γ_2 . This is illustrated in Figure 2 below.

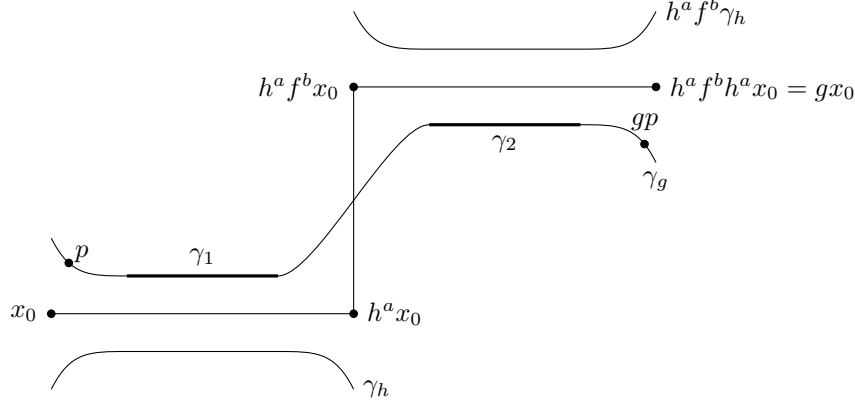


Figure 2: The axis γ_g fellow travels two translates of γ_h .

Let p be a closest point on γ_g to the basepoint x_0 . If an element g' in G K -coarsely stabilizes $[p, gp]$, then g' $(K + O(\delta))$ -stabilizes γ_1 and γ_2 . The segments γ_1 and γ_2 fellow travel axes of two distinct translates of γ_h , say $u_1\gamma_h$ and $u_2\gamma_h$, and so g' $(K + O(\delta))$ -stabilizes segments of these axes of length at least D_h . Therefore by Lemma 21, g' lies in

$$E(u_1 h u_1^{-1}) \cap E(u_2 h u_2^{-1}),$$

which is equal to

$$(u_1 \langle h \rangle u_1^{-1} \rtimes E(G)) \cap (u_2 \langle h \rangle u_2^{-1} \rtimes E(G)),$$

as h is weakly asymmetric. Hyperbolic elements in each of these subgroups have distinct fixed points in ∂X , and so cannot be equal. The set of non-hyperbolic elements is equal to $E(G)$, therefore the intersection of the two subgroups is exactly $E(G)$, and so $g' \in E(G)$, as required. \square

Finally, we show that these geometric conditions are sufficient to show that a group element g is weakly asymmetric.

Proposition 22. *Let G be a countable group acting acylindrically hyperbolically on the separable space X . Then there is a constant K , depending only on δ , such that if g is an element which is hyperbolic, K -primitive, K -asymmetric and irreversible, then g is weakly asymmetric.*

Proof. Let g be a group element in G which is hyperbolic, irreversible, K -primitive and K -asymmetric, and let h be an element of $E(g)$. Let α_g be an axis for g , and let p be a closest point on α_g to the basepoint x_0 . As g is K -primitive, we may multiply by a power of g , so that $g^n h$ K -coarsely fixes $[p, gp]$. As g is K -asymmetric, this implies that $g^n h$ lies in $E(G)$, and so h lies in $\langle g \rangle E(G)$. Finally, as g is hyperbolic, $\langle g \rangle E(G)$ is a semidirect product $\langle g \rangle \ltimes E(G)$, by Proposition 2. \square

5.2 Random elements are asymmetric

In this section we show that the geometric properties defined in the previous section hold for random elements w_n with asymptotic probability one.

We start by showing that the translation length $\tau(w_n)$ also grows linearly, using Proposition 14.

Lemma 23. *Let G be a countable group acting acylindrically hyperbolically on the separable space X , and let μ be an admissible probability distribution on G . For any $0 < \varepsilon < 1$ the probability that $\tau(w_n) \geq (1 - \varepsilon) |\gamma_n|$ goes to 1.*

Notice that, in the notation of the lemma, $|\gamma_n| \geq \tau(w_n)$ always holds.

Proof. We shall apply Proposition 14 with $g = w_n$, considered as a product of $g_1 = w_m$ and $g_2 = w_m^{-1} w_n$, where $m = \lfloor n/2 \rfloor$. Recall that $w_n = s_1 \dots s_n$, where the s_i are the steps of the random walk, and are independent μ -distributed random variables.

By linear progress, Proposition 9.1, there exists $L > 0$ such that both $\mathbb{P}(d_X(x_0, w_m x_0) \geq Ln)$ and $\mathbb{P}(d_X(x_0, w_m^{-1} w_n x_0) \geq Ln)$ tend to one as n tends to infinity (the L here is smaller than the L in Proposition 9.1).

By Proposition 9.2, the probability that the Gromov product $(w_m^{-1} x_0 \cdot w_m^{-1} w_n x_0)_{x_0} = (x_0 \cdot w_n x_0)_{w_m x_0}$ is bounded above by $\varepsilon Ln/5$ tends to one as n tends to infinity. For the other Gromov product $((w_m^{-1} w_n)^{-1} x_0 \cdot w_m x_0)_{x_0}$, the two random variables $(w_m^{-1} w_n)^{-1} = s_n^{-1} \dots s_{m+1}^{-1}$ and $w_m = s_1 \dots s_m$ are independent, and so the distribution of

$$((w_m^{-1} w_n)^{-1} x_0 \cdot w_m x_0)_{x_0} = (s_n^{-1} \dots s_{m+1}^{-1} x_0 \cdot s_1 \dots s_m x_0)_{x_0}$$

is the same as the distribution of

$$(s_{n-m}^{-1} \dots s_1^{-1} x_0 \cdot s_{n-m+1} \dots s_n x_0)_{x_0} = (x_0 \cdot w_n x_0)_{w_{n-m} x_0},$$

and so again by Proposition 9.2, the probability that this Gromov product is bounded above by $\varepsilon Ln/5$ tends to one as n tends to infinity.

Therefore, the probability that the two inequalities (7) are satisfied tends to one as n tends to infinity. Hence, by Proposition 14, for n

sufficiently large we have $\tau(w_n) \geq d_X(x_0, w_n x_0) + d_X(w_n x_0, w_n^2 x_0) - \varepsilon L n \geq (1 - \varepsilon)|\gamma_n|$ with probability that tends to 1 as n tends to infinity, as required. \square

We now show that the probability that w_n is irreversible tends to one as n tends to infinity.

Proposition 24. *Let G be a countable group acting acylindrically hyperbolically on the separable space X , and let μ be an admissible probability distribution on G . Then for any K , the probability that w_n is irreversible tends to one as n tends to infinity.*

Proof. We can assume that w_n is hyperbolic, with axis α_n . Now suppose $h \in E(w_n)$ is an element which reverses the endpoints of w_n . Since α_n and $h\alpha_n$ are $O(\delta)$ -fellow travelers, this gives a $(\frac{1}{2}\tau(w_n) - O(\delta), O(\delta))$ -match for any subsegment of α_n of length $\tau(w_n)$.

Propositions 10.2 and 10.5 (in view of Lemma 23) then show that the probability that this occurs tends to zero as n tends to infinity.

In fact, informally, if α_n had a match of size approximately $\tau(w_n)/2$, then by Proposition 10.5 the same would be true of γ_n , but this is ruled out by Proposition 10.2 since Lemma 23 says that $\tau(w_n)$ is approximately equal to $|\gamma_n|$. \square

We now show that random walks give K -primitive elements with asymptotic probability one.

Proposition 25. *Let G be a countable group acting acylindrically hyperbolically on the separable space X , and let μ be an admissible probability distribution on G . Then for any K , the probability that w_n is K -primitive tends to one as n tends to infinity.*

Proof. Let α_g be an axis for a hyperbolic element with $\tau(g) > K + O(\delta)$, and suppose there is an element h in $E(g)$ which does not K -stabilize P . Up to replacing h with some $g^k h$, we can assume $d_X(p_0, hp_0) \leq \frac{1}{2}d_X(p_0, gp_0) + O(\delta)$. As h moves p_0 distance at least K , h is hyperbolic by applying Proposition 14, in the case where $n = 1$, $g = g_1 = h$ and the basepoint $x_0 = p_0$. Therefore, there is a power of h such that

$$\frac{1}{3}d_X(p_0, gp_0) - O(\delta) \leq d_X(p_0, h^a p_0) \leq \frac{1}{2}d_X(p_0, gp_0) + O(\delta).$$

As α_g and $h^a \alpha_g$ are $O(\delta)$ -fellow travelers, this gives a $(\frac{1}{3}\tau(g) - O(\delta), O(\delta))$ -match for any subsegment of α_g of length $\tau(g)$. Proposition 10.5 then implies that the probability that γ_n has a $(\frac{1}{3}\tau(g) - O(\delta), O(\delta))$ -match tends to one as n tends to infinity, and the probability that this occurs tends to zero as n tends to infinity, by Proposition 10.2. \square

We now show that the probability that w_n is K -asymmetric tends to one as n tends to infinity.

Proposition 26. *Let G be a countable group acting acylindrically hyperbolically on the separable space X , and let μ be an admissible probability distribution on G . Then for any constant $K \geq 0$ the probability that w_n is K -asymmetric tends to one as n tends to infinity.*

Proof. By Proposition 25 the probability that w_n is hyperbolic and K -primitive tends to one as n tends to infinity. By Proposition 20 there is an element h in the support of μ which is $(K + O(\delta))$ -asymmetric. Let α_h be an axis for h , and let p be a closest point on α_h to the basepoint x_0 . Then Proposition 10.4 implies that the probability that w_n is hyperbolic with axis α_n , and α_n has a subsegment of length at least $2\tau(h)$ which $O(\delta)$ -fellow travels with a translate of α_h tends to one as n tends to infinity. If this happens, then if an element $g \in G$ K -stabilizes $[x_0, w_n x_0]$, then it also $(K + O(\delta))$ -stabilizes a translate of $[p, hp]$. As h is $(K + O(\delta))$ -asymmetric, this implies that $g \in E(G)$, so w_n is K -asymmetric, as required. \square

This completes the proof of Proposition 16: we have shown that all of the geometric hypotheses of Proposition 22 hold with asymptotic probability one, so Proposition 22 implies that w_n is hyperbolic and weakly asymmetric with asymptotic probability one.

Although we have completed the proof of the special case of Theorem 5 in the case $k = 1$, we now conclude this section by showing a slightly stronger result, which we will need for the general case.

Proposition 27. *Let G be a countable group acting acylindrically hyperbolically on the separable space X , and let μ be an admissible probability distribution on G with positive drift $L > 0$. Let $0 < \varepsilon < \frac{1}{6}$. Then the probability that w_n is (εLn) -asymmetric tends to 1 as n tends to infinity.*

Proof. Let h be a hyperbolic element in the support of μ which is $K = O(\delta)$ -asymmetric, with axis α_h , and let p be a closest point on α_h to the basepoint x_0 .

The probability that w_n is hyperbolic tends to one, so we may assume that w_n is hyperbolic with axis α_n . Let q be a closest point on α_n to x_0 , let γ be a geodesic from q to $w_n q$, and let g be a group element which (εLn) -coarsely stabilizes γ . We have already shown the result for group elements g which K -stabilize γ for fixed K , so we may assume that $d_X(q, gq)$ and $d_X(w_n q, gw_n q)$ are both at least $K = O(\delta)$.

We now show that there is a subgeodesic γ^- of γ for which all points are moved a similar distance by g . Define γ^- to be $\gamma \setminus (B_X(q, 2\varepsilon Ln) \cup B_X(w_n q, 2\varepsilon Ln))$.

Claim 28. For all s and t in γ^- ,

$$|d_X(s, gs) - d_X(t, gt)| \leq O(\delta).$$

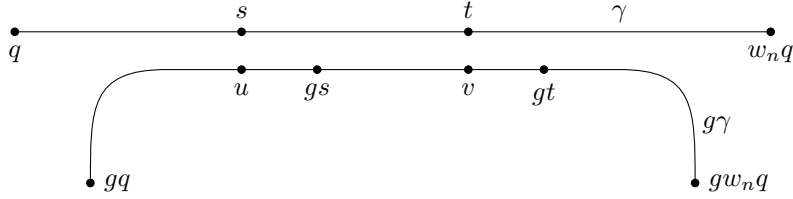


Figure 3: Points on γ^- are moved a similar distance.

Proof. As g is an isometry $d_X(s, t) = d_X(gs, gt)$. Let u be a closest point on $g\gamma$ to s , and let v be a closest point on $g\gamma$ to t , then $d_X(u, v) = d_X(s, t) + O(\delta)$. This implies that $d_X(u, gs) = d_X(v, gt) + O(\delta)$, and as $d_X(u, s) \leq 2\delta$ and $d_X(v, t) \leq 2\delta$, thus implies that $d_X(s, gs) = d_X(t, gt) + O(\delta)$, as required. \square

By Propositions 9.1 and 10.3 the length of γ is at least $(1 - \varepsilon)Ln$, and so the length of γ^- is at least $(1 - 3\varepsilon)Ln$. Therefore by Proposition 10.4 the probability that γ^- has a subsegment of length at least $2\tau(h)$ which $O(\delta)$ -fellow travels with γ_h tends to 1 as n tends to infinity. If $d_X(s, gs) \leq K = O(\delta)$ for $s \in \gamma^-$, then $g(K + O(\delta))$ -stabilizes a translate of $[p, hp]$, and so $g \in E(G)$, which implies that w_n is K -asymmetric, as required. Therefore the final step is to eliminate the case in which $d_X(s, gs) \geq K = O(\delta)$ for $s \in \gamma^-$, which we now consider.

Let s be a point on γ^- , let t be a nearest point to gs on γ , and let u be a nearest point on γ to gt . This is illustrated below in Figure 4.

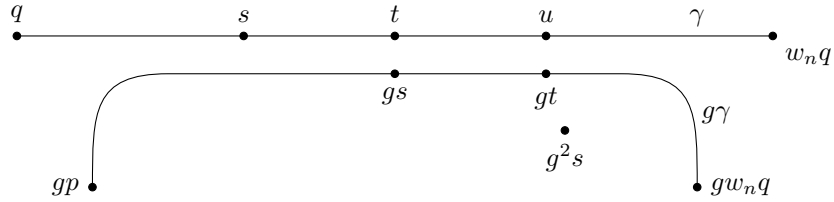


Figure 4: The image of s under g and g^2 .

The distance from gs to t is at most 2δ , and the distance from $g^2 s$ to u is at most 4δ . As $d_X(s, gx) \geq K = O(\delta)$, this gives an upper bound

on the Gromov product $(s \cdot g^2 s)_{gs} = (g^{-1} s \cdot gs)_s$ of at most $O(\delta)$, and so we may apply Proposition 15. Therefore, g is hyperbolic, and the axis α_g for g passes within distance $O(\delta)$ of t . Furthermore, this holds for all $t \in \gamma^-$, so the axis α_g for g $O(\delta)$ -fellow travels with γ^- . The axis α_g is $\tau(g)$ periodic, and $\tau(g) \leq \varepsilon Ln$, this means that γ^- , and hence γ_n has an $(\varepsilon Ln + O(\delta), O(\delta))$ -match, which contradicts Proposition 10.2. \square

6 General case: many generators

We briefly recall the notation we use for a random subgroup $H = H(\mu_i, n_i)$. The μ_1, \dots, μ_k are admissible probability distributions on G , and the n_1, \dots, n_k are positive integers. We write w_{i, n_i} for a random walk of length n_i generated by the probability distribution μ_i , and γ_i for a geodesic in X from x_0 to $w_{i, n_i} x_0$. We shall write H for the subgroup generated by $\{w_{1, n_1}, \dots, w_{k, n_k}\}$, and set $n = \min n_i$. Recall that the random walk generated by an admissible probability distribution μ_i has positive drift, i.e. there is a constant L_i such that $\frac{1}{n} d_X(x_0, w_{i, n_i} x_0) \rightarrow L_i$ as $n_i \rightarrow \infty$, almost surely. We shall set $L = \min L_i$, so in particular $L > 0$, and we shall reorder the μ_i so that $Ln \leq L_1 n_1 \leq \dots \leq L_k n_k$, as we shall need to keep track of the expected lengths of the generators in the subsequent argument. Finally, it will be convenient to have notation for paths which travel along a geodesic γ_i in the reverse direction, so we will extend our index set from $I = \{1, \dots, k\}$ to $\pm I = \{\pm 1, \dots, \pm k\}$, and write γ_{-i} for a geodesic in X from x_0 to $w_{i, n_i}^{-1} x_0$, which is a translate by w_{i, n_i}^{-1} of the reverse path along γ_i .

In order to show that H is hyperbolically embedded in G we shall show that H is freely generated by $\{w_{1, n_1}, \dots, w_{k, n_k}\}$, H is quasi-isometrically embedded in X , and $H \rtimes E(G)$ is geometrically separated, with asymptotic probability one.

We start by showing some generalizations of the properties that hold for individual random walks to the case of multiple random walks. Each individual random walk makes linear progress with exponential decay. We now show that the collection of k random walks also makes linear progress with exponential decay.

Definition 29. Given $0 < \varepsilon < 1$, and a random subgroup H , we say that H satisfies ε -length bounds if

$$(1 - \varepsilon)L_i n_i \leq d_X(x_0, w_{i, n_i} x_0) \leq (1 + \varepsilon)L_i n_i. \quad (10)$$

for all $1 \leq i \leq k$.

Proposition 30. Let H be a random subgroup, and let $\varepsilon > 0$. Then there are constants K and c , depending only on ε , and the probability dis-

tributions μ_i , such that the probability that a random subgroup H satisfies ε -length bounds is at least $1 - Kc^n$.

Proof. By Proposition 9.1, for any $\varepsilon > 0$, for each μ_i there are constants L_i, K_i and c_i such that

$$\mathbb{P}((1 - \varepsilon)L_i n_i \leq d_X(x_0, w_{i, n_i} x_0) \leq (1 + \varepsilon)L_i n_i) \geq 1 - K_i c_i^{n_i}.$$

If $K' = \max K_i$, $c = \max c_i$ and $n = \min n_i$, then the probability that these inequalities are satisfied simultaneously for all i is at least $1 - kKc^n$. Therefore the required estimate holds, with $K = kK'$, and the previous choice of c . \square

We now show that the collection of k random walks satisfies the following estimates on their mutual Gromov products.

Definition 31. We say a random subgroup H satisfies K -Gromov product bounds if

$$(ax_0 \cdot bx_0)_{x_0} \leq K.$$

for all distinct a and b in the symmetric generating set $A = \{w_{1, n_1}^{\pm 1}, \dots, w_{k, n_k}^{\pm 1}\}$ for H .

Proposition 32. Let H be a random subgroup. Given $0 < \varepsilon < \frac{1}{2}$ there are constants K and c , depending only on ε , and the probability distributions μ_i , such that the probability that H satisfies (εLn) -Gromov product bounds is at least $1 - Kc^n$.

Proof. If $(ax_0 \cdot bx_0)_{x_0} \leq \varepsilon Ln$, then, by definition of shadows, $ax_0 \in S_{x_0}(bx_0, d_X(x_0, bx_0) - \varepsilon Ln)$. By Proposition 9.3, the random walk determined by each μ_i satisfies exponential decay for shadows, i.e. there are constants R_0, K_i and $c_i < 1$ such that for all $R \geq R_0$, and all $g \in G$,

$$\mathbb{P}(w_{i, n_i} \in S_{x_0}(gx_0, R)) \leq K_i c_i^{d_X(x_0, gx_0) - R}. \quad (11)$$

We shall use (11) with $g = b$. If

$$d_X(x_0, bx_0) - \varepsilon Ln \geq R_0, \quad (12)$$

then (11) implies that the probability that $(ax_0 \cdot bx_0)_{x_0} \leq \varepsilon Ln$ is at most $K_i c_i^{\varepsilon Ln}$.

In order to apply the estimate (11), we need to check that (12) holds with asymptotic probability one. Using linear progress, Proposition 9.1,

$$\mathbb{P}(d_X(x_0, bx_0) \leq (1 - \varepsilon)Ln) \leq K'_i c_i'^n,$$

for some constants K'_i and c'_i depending on ε and μ_i . Therefore

$$\mathbb{P}(d_X(x_0, bx_0) - \varepsilon Ln \leq (1 - 2\varepsilon)Ln) \leq K'_i c_i'^n.$$

As we have chosen $\varepsilon < \frac{1}{2}$, this implies that

$$\mathbb{P}(d_X(x_0, bx_0) - \varepsilon Ln \leq R_0) \leq K'_i c_i'^n.$$

for all $n \geq R_0/(L(1 - 2\varepsilon))$.

Therefore, the probability that $(ax_0 \cdot bx_0)_{x_0} \leq \varepsilon Ln$ is at most $K'_i c_i'^n + K_i c_i^{\varepsilon Ln}$. As there are at most $2k$ choices for each of a and b in A , the probability that any of these events occurs is at most $4k^2 K'' c^n$, where $K'' = \max\{K_i, K'_i\}$ and $c_i = \max\{c_i, c'_i\}$. The result then holds with $K = 4k^2 K''$, and the previous choice of c , as required. \square

If H satisfies ε -length bounds and (εLn) -Gromov product bounds, then the conditions (9) are satisfied in Proposition 15, so the rescaled Cayley graph Γ_H is $(6, O(\varepsilon Ln))$ -quasi-isometrically embedded in X . In particular, this implies that H is freely generated by $\{w_{1,n_1}, \dots, w_{k,n_k}\}$, and $HE(G)$ is a semidirect product $H \ltimes E(G)$. As well as these properties, it will be convenient to know certain matching properties for the geodesics defined by H , which we now describe.

Definition 33. We say that a random subgroup H has an ε -large match if a translate of $[\gamma_j(\varepsilon Ln), \gamma_j(|\gamma_j| - \varepsilon Ln)]$ is contained in a 2δ -neighbourhood of γ_i , for some $i < j$.

Proposition 34. Let H be a random subgroup, and let $0 < \varepsilon < \frac{1}{3}$. Then there are constants K and c , depending on ε and the probability distributions μ_i , such that the probability that H has an ε -large match is at most Kc^n .

Proof. We may assume that H satisfies ε -length bounds, which by Proposition 30, happens with probability at least $1 - K'c'^n$, for some K' and $c' < 1$, depending on the μ_i and ε . By ε -length bounds, the length of γ_j is at least $(1 - \varepsilon)L_j n_j$, and the length of γ_i is at most $(1 + \varepsilon)L_i n_i$.

Let γ_j^- be the subgeodesic of γ_j given by $[\gamma_j(\varepsilon Ln), \gamma_j(|\gamma_j| - \varepsilon Ln)]$. It will be convenient to consider a discrete set of points $\gamma_j(\ell)$ along γ_j , where $\ell \in \mathbb{N}$. If γ_j^- is contained in a 2δ -neighbourhood of $[\gamma_i(t), \gamma_i(t + |\gamma_j^-|)]$, then γ_j^- is contained in a $(2\delta + 1)$ -neighbourhood of $[\gamma_i(\ell), \gamma_i(\ell + |\gamma_j^-|)]$ for some $\ell \in \mathbb{N}$.

By Proposition 10.1, there are constants K_i and $c_i < 1$ such that the probability that a translate of γ_j^- is contained in a $(2\delta + 1)$ -neighbourhood of γ_i starting at $\gamma_i(\ell)$ is at most

$$K_i c_i^{(1-\varepsilon)L_j n_j - 2\varepsilon Ln} \leq K c^{(1-3\varepsilon)L_j n_j},$$

where the inequality above holds with $K = \max K_i$, $c = \max c_i$, and $Ln \leq L_j n_j$. Given the length estimates for γ_i and γ_j , the number of

possible values of ℓ is at most

$$(1 + \varepsilon)L_i n_i - (1 - \varepsilon)L_j n_j + 2\varepsilon L n \leq 3\varepsilon L_j n_j,$$

where the inequality holds as $L_i n_i \leq L_j n_j$, and negative terms on the left hand side are discarded.

Therefore, the probability that a translate of γ_j^- is contained in a 2δ -neighbourhood of γ_i is at most

$$3\varepsilon L_j n_j K c^{(1-3\varepsilon)L_j n_j} \leq K'' c'^n,$$

for some constants K'' and c'' , where the inequality above holds as the function $f(x) = x c^x$ is decreasing for all x sufficient large, and bounded above by a constant multiple of an exponential function. As there are at most $2k$ choices of indices for each of i and j , the result follows. \square

Finally, we give an estimate for the probability that a geodesic γ_j has an initial segment which matches a terminal segment of γ_i , concatenated with an initial segment of $\gamma_{i'}$, for some $i \leq j$ and $i' \leq j$.

Given a collection of geodesics $\{\gamma_i\}_{i \in \pm I}$, and a number K , define a collection of geodesic segments $\{\eta(i, i', K, \ell) \mid i, i' \in \pm I, i \neq -i', \ell \in \mathbb{N}, 0 \leq \ell \leq |\gamma_i|\}$ as follows. Let i and i' be indices in $\pm I$ with the property that $i \neq -i'$, and let $0 \leq \ell \leq |\gamma_i|$ be an integer. Let p be a point on γ_i distance ℓ from its endpoint, and let q be a point on $w_i \gamma_{i'}$ distance K from the initial point of $w_i \gamma_{i'}$. Define $\eta(i, i', K, \ell)$ to be a geodesic from p to q .

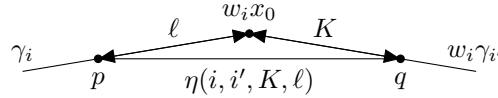


Figure 5: A geodesic $\eta(i, i', K, \ell)$.

Definition 35. We say that a random subgroup H is K -unmatched if for all $i \leq j$, $i' \leq j$ and for $0 \leq t \leq K$, no geodesic $\eta(i, i', K, \ell)$, is contained in a 2δ -neighbourhood of a subgeodesic of γ_j starting at $\gamma_j(t)$.

Proposition 36. Let H be a random subgroup, and let $0 < \varepsilon < \frac{1}{6}$. Then there are constants K and c , depending on ε and the μ_i , such that the probability that H is $(3\varepsilon L n)$ -unmatched is at least $1 - K c^n$.

Proof. We shall assume that the random subgroup H satisfies the ε -length bounds and $(\varepsilon L n)$ -Gromov product bounds, which happens with probability at least $1 - K' c'^n$, for some constants K' and c' , depending on ε and the μ_i .

First consider a fixed collection of indices i, i', j in $\pm I$, with $i \leq j$, $i' \leq j$ and $i \neq -i'$. The Gromov product bound for i and i' implies that the length of $\eta = \eta(i, i', 3\varepsilon Ln, \ell)$ is at least $\ell + 3\varepsilon Ln - 2\varepsilon Ln = \ell + \varepsilon Ln$. If a translate of $\eta(i, i', 3\varepsilon Ln, \ell)$ is contained in a 2δ neighbourhood of $[\gamma_j(t), \gamma_j(t + |\eta|)]$, then it is contained in a $(2\delta + 1)$ -neighbourhood of $[\gamma_j(m), \gamma_j(m + |\eta|)]$, for some $m \in \mathbb{N}$.

By Proposition 10.1, the probability that a translate of $\eta(i, i', 3\varepsilon Ln, \ell)$ is contained in a $(2\delta + 1)$ -neighbourhood of $[\gamma_j(m), \gamma_j(m + |\eta|)]$ is at most $Kc^{\ell + \varepsilon Ln}$. As there are at most $3\varepsilon Ln$ choices for m , the probability that this occurs for some $0 \leq m \leq 3\varepsilon Ln$ is at most $3\varepsilon Ln Kc^{\ell + \varepsilon Ln}$. The sum of these probabilities over all values of ℓ is at most $(3\varepsilon Ln Kc^{\varepsilon Ln})/(1 - c) \leq K'c^n$ for different constants K' and c' .

There are at most $2k$ possible admissible choices for each of the indices i, i' and j , and so assuming ε -length bounds and Gromov product bounds, the probability that the geodesics are not $(3\varepsilon Ln)$ -unmatched is at most $(2k)^3 K'c^n$. Therefore, the probability that ε -length bounds, Gromov bounds and $(3\varepsilon Ln)$ -unmatching all hold simultaneously is at least $1 - Kc'^n$, for $K = (2k)^3 K'$. \square

In order to show Theorem 5 it therefore suffices to show:

Proposition 37. *Let H be a random subgroup of G , and let $0 < \varepsilon < \frac{1}{6}$. If H satisfies ε -length bounds, (εLn) -Gromov product bounds, has no ε -large match and is $(3\varepsilon Ln)$ -unmatched, then Γ_H is $(6, O(\delta, \varepsilon Ln))$ -quasi-isometrically embedded in X and $H \rtimes E(G)$ is geometrically separated in X .*

We now prove Theorem 5, assuming Proposition 37.

Proof (of Theorem 5). The first property in Theorem 5, the fact that each generator w_{i, n_i} is hyperbolic and asymmetric, follows from Proposition 16 applied to each of the random walks w_{i, n_i} .

The second property, that Γ_H is a quasi-isometrically embedded follows (as we have already observed) if H satisfies ε -length bounds and (εLn) -Gromov product bounds, which hold with probabilities at least $1 - Kc^n$, by Propositions 30 and 32, for constants K and $c < 1$ depending only on ε and the μ_i . This then implies that H is freely generated by its generators w_{i, n_i} and $HE(G) = H \rtimes E(G)$.

The final property, that $H \rtimes E(G)$ is geometrically separated, holds if H satisfies the four conditions, ε -length bounds, (εLn) -Gromov product bounds, no ε -large match and being $(3\varepsilon Ln)$ -unmatched, and these hold with probability at least $1 - K'c'^n$, by Propositions 30, 32, 34 and 36, for some constants K' and $c' < 1$, depending only on ε and the μ_i , as required. \square

The final step is to prove Proposition 37. We shall use the following properties of geodesics and quasigeodesics in a hyperbolic space X , see for example Bridson and Haefliger [BH99, III.H.1]. If two geodesics in X are A -fellow travellers, then they are in fact $O(\delta)$ -fellow travellers, outside balls of radius A about their endpoints. Similarly, if two (A, B) -quasigeodesics are C -fellow travellers, then they are $O(\delta, A, B)$ -fellow travellers outside C -neighbourhoods of their endpoints.

Proof (of Proposition 37). Recall that the (image in X of the) rescaled Cayley graph Γ_H is the union of translates of geodesic segments γ_i from x_0 to $w_{i,n_i}x_0$ by elements of H . Let γ be a geodesic in X connecting two points h_1x_0 and h_2x_0 of Hx_0 . These two points are also connected by a path $\hat{\gamma}$ in Γ_H , which is a concatenation of geodesic segments γ_i , corresponding to the reduced word determined by $h_1^{-1}h_2$ in H . The path $\hat{\gamma}$ is an $(6, O(\delta, \varepsilon Ln))$ -quasigeodesic in X , which by the Morse property is contained in an $O(\delta, \varepsilon Ln)$ -neighbourhood of γ .

We will show that geometric separation holds for a constant $B(R) = 4R + O(\delta, \varepsilon Ln)$. Let γ and γ' be geodesics in X of length at least B , with endpoints in H , and an element $g \in G$, such that $g\gamma$ is an $(2R + O(\delta))$ -fellow traveller with γ' . In order to show geometric separation, it suffices to show that g in fact lies in $H \rtimes E(G)$.

Let $\hat{\gamma}$ and $\hat{\gamma}'$ be the corresponding paths in Γ_H connecting the endpoints of γ and γ' . The quasigeodesics $\hat{\gamma}$ and $\hat{\gamma}'$ are $(2R + O(\delta, \varepsilon Ln))$ -fellow travellers in X , and we shall denote their endpoints by $\hat{\gamma}(0)$ and $\hat{\gamma}(T)$ for $\hat{\gamma}$, and $\hat{\gamma}'(0)$ and $\hat{\gamma}'(T')$ for $\hat{\gamma}'$. Therefore, if we set $\hat{\gamma}_-$ and $\hat{\gamma}'_-$ to be the largest union of segments which are translates of the γ_i contained in $\hat{\gamma} \setminus (B_X(\hat{\gamma}(0) \cup \hat{\gamma}(T), 2R + O(\delta, \varepsilon Ln)))$ and $\hat{\gamma}' \setminus (B_X(\hat{\gamma}'(0) \cup \hat{\gamma}'(T'), 2R + O(\delta, \varepsilon Ln)))$, then $\hat{\gamma}_-$ and $\hat{\gamma}'_-$ are $O(\delta, \varepsilon Ln)$ -fellow travellers. By a sufficiently large choice of B we may assume that the lengths of $\hat{\gamma}$ and $\hat{\gamma}'$ are at least $4R + (1 + \varepsilon)Ln + O(\delta)$, and so both $\hat{\gamma}_-$ and $\hat{\gamma}'_-$ are non-empty, as we have assumed that the γ_i satisfy ε -length bounds and Gromov product bounds.

Each path $\hat{\gamma}_-$ or $\hat{\gamma}'_-$ is a concatenation of geodesic segments which are translates of the γ_i . Let j be the largest index of any path segment whose translate appears in either of $\hat{\gamma}_-$ or $\hat{\gamma}'_-$. If the largest index j does not appear in both paths, then up to relabelling, we may assume that j occurs in $\hat{\gamma}_-$, and let $h\gamma_j$ be a corresponding geodesic segment in the path $\hat{\gamma}_-$, for some $h \in H$.

We now consider two cases. Either the nearest point projection of $h\gamma_j$ to $\hat{\gamma}_-$ is contained in the translate of a single γ_i for $i \leq j$, or $h\gamma_j \subset \hat{\gamma}_-$ contains a point within distance εLn of some point of the orbit Hx_0 . If the first case occurs with $i < j$, then H has an ε -large match, which we have

assumed does not happen, so $gh\gamma_j$ in fact (εLn) -fellow travels a translate of itself in $\widehat{\gamma}_-$. This means that the translate $gh\gamma_j$ (εLn) -fellow travels $h'\gamma_j$ for some $h' \in H$, and so $h'^{-1}gh$ $(\varepsilon Ln + O(\delta))$ -stabilizes $[p, w_{j,n_j}p]$, where p is a nearest point projection of the basepoint x_0 to the axis α_j for w_{j,n_j} . By Proposition 24, w_{j,n_j} is irreversible with asymptotic probability one, so $h'^{-1}gh$ does swap the endpoints of the geodesic $[p, w_{j,n_j}p]$, and by Proposition 27, we may assume that w_{j,n_j} is $(\varepsilon Ln + O(\delta))$ -asymmetric, and so this implies that $h'^{-1}gh \in \langle w_{j,n_j} \rangle \rtimes E(G) \subset H \rtimes E(G)$. As both h and h' lie in H , this implies that g lies in $H \rtimes E(G)$, with asymptotic probability one, as required.

It remains to show that if the second case occurs then H is $(3\varepsilon Ln)$ -unmatched, as we now explain. Let p be a point in Γ_H closest to the initial point of $g'\gamma_j$, and let q be the point in Γ_H closest to the terminal point of $g'\gamma_j$. Let hx_0 be the first point of Hx_0 occurring between p and q . Let $hw_i^{-1}\gamma_i$ be the geodesic segment of Γ_H containing p , and let $h\gamma_{i'}$ be the next geodesic segment of Γ_H along the geodesic in Γ_H from p to q . Finally, let q' be a point on $h\gamma_{i'}$ distance εLn from hx_0 . This is illustrated below in Figure 6.

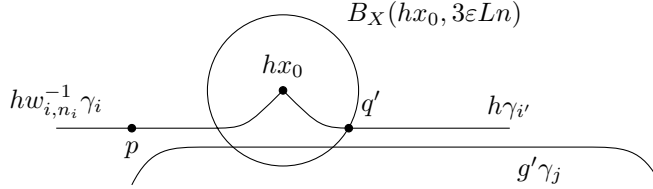


Figure 6: A subsegment of the geodesic $g\widehat{\gamma}_-$ fellow travels Γ_H .

We now observe that the geodesic in X from p to q' is the geodesic $\eta(i, i', 3\varepsilon Ln\ell)$ used in Definition 35, and so if the second case occurs, then H is not (εLn) -unmatched, contradicting our initial assumptions on H . \square

References

- [AMS16] Yago Antolin, Ashot Minasyan, and Alessandro Sisto, *Commensurating endomorphisms of acylindrically hyperbolic groups and applications*, Groups, Geometry, and Dynamics, to appear (2016).
- [Aou11] Richard Aoun, *Random subgroups of linear groups are free*, Duke Math. J. **160** (2011), no. 1, 117–173.

- [BGH16] Hyungryul Baik, Ilya Gekhtman, and Ursula Hamenstädt, *The smallest positive eigenvalue of fibered hyperbolic 3-manifolds* (2016), available at [arXiv:1608.07609](#).
- [BHS14] Jason Behrstock, Mark Hagen, and Alessandro Sisto, *Hierarchically hyperbolic spaces I: curve complexes for cubical groups* (2014), available at [arXiv:1412.2171](#).
- [BF14] Mladen Bestvina and Mark Feighn, *Hyperbolicity of the complex of free factors*, Adv. Math. **256** (2014), 104–155.
- [BF02] Mladen Bestvina and Koji Fujiwara, *Bounded cohomology of subgroups of mapping class groups*, Geom. Topol. **6** (2002), 69–89 (electronic).
- [Bow06] Brian H. Bowditch, *Intersection numbers and the hyperbolicity of the curve complex*, J. Reine Angew. Math. **598** (2006), 105–129.
- [BH99] Martin R. Bridson and André Haefliger, *Metric spaces of non-positive curvature*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 319, Springer-Verlag, Berlin, 1999.
- [CM15] Danny Calegari and Joseph Maher, *Statistics and compression of scl*, Ergodic Theory Dynam. Systems **35** (2015), no. 1, 64–110.
- [CM16] Indira Chatterji and Alexandre Martin, *A note on the acylindrical hyperbolicity of groups acting on $CAT(0)$ cube complexes* (2016), available at [arXiv:1610.06864](#).
- [DH15] F. Dahmani and C. Horbez, *Spectral theorems for random walks on mapping class groups and $Out(F_N)$* (2015), available at [arXiv:1506.06790](#).
- [DGO11] F. Dahmani, V. Guirardel, and D. Osin, *Hyperbolically embedded subgroups and rotating families in groups acting on hyperbolic spaces* (2011), available at [arXiv:1111.7048](#).
- [FM12] Benson Farb and Dan Margalit, *A primer on mapping class groups*, Princeton Mathematical Series, vol. 49, Princeton University Press, Princeton, NJ, 2012.
- [FPS15] R. Frigerio, M. B. Pozzetti, and A. Sisto, *Extending higher-dimensional quasi-cocycles*, J. Topol. **8** (2015), no. 4, 1123–1155.
- [GM16] Vaibhav Gadre and Joseph Maher, *The stratum of random mapping classes* (2016), available at [arXiv:1607.01281](#).
- [Gen16] Anthony Genevois, *Contracting isometries of $CAT(0)$ cube complexes and acylindrical hyperbolicity of diagram groups* (2016), available at [arXiv:1610.07791](#).
- [GMO10] Robert Gilman, Alexei Miasnikov, and Denis Osin, *Exponentially generic subsets of groups*, Illinois J. Math. **54** (2010), no. 1, 371–388.
- [Gro87] M. Gromov, *Hyperbolic groups*, Essays in group theory, Math. Sci. Res. Inst. Publ., vol. 8, Springer, New York, 1987, pp. 75–263.

- [Gro03] M. Gromov, *Random walk in random groups*, Geom. Funct. Anal. **13** (2003), no. 1, 73–146.
- [GS16] Dominik Gruber and Alessandro Sisto, *Infinitely presented graphical small cancellation groups are acylindrically hyperbolic* (2016), available at [arXiv:1408.4488](#).
- [Gui90] Yves Guivarc’h, *Produits de matrices aléatoires et applications aux propriétés géométriques des sous-groupes du groupe linéaire*, Ergodic Theory Dynam. Systems **10** (1990), no. 3, 483–512.
- [Ham08] Ursula Hamenstädt, *Bounded cohomology and isometry groups of hyperbolic spaces*, J. Eur. Math. Soc. (JEMS) **10** (2008), no. 2, 315–349.
- [HS16] Tobias Hartnick and Alessandro Sisto, *work in progress* (2016).
- [Hea16] Burns Healy, *CAT(0) Groups and Acylindrical Hyperbolicity* (2016), available at [arXiv:1610.08005](#).
- [Hul13] Michael Hull, *Small cancellation in acylindrically hyperbolic groups* (2013), available at [arXiv:1308.4345](#).
- [HO13] Michael Hull and Denis Osin, *Induced quasicycles on groups with hyperbolically embedded subgroups*, Algebr. Geom. Topol. **13** (2013), no. 5, 2635–2665.
- [Jit02] Toshiaki Jitsukawa, *Malnormal subgroups of free groups*, Computational and statistical group theory (Las Vegas, NV/Hoboken, NJ, 2001), Contemp. Math., vol. 298, Amer. Math. Soc., Providence, RI, 2002, pp. 83–95.
- [MT14] Joseph Maher and Giulio Tiozzo, *Random walks on weakly hyperbolic groups* (2014), available at [arXiv:1410.4173](#).
- [MTV] Armando Martino, Ted Turner, and Enric Ventura, *The density of injective endomorphisms of a free group*.
- [Mas14] Hidetoshi Masai, *Fibered commensurability and arithmeticity of random mapping tori* (2014), available at [arXiv:1408.0348](#).
- [MM99] Howard A. Masur and Yair N. Minsky, *Geometry of the complex of curves. I. Hyperbolicity*, Invent. Math. **138** (1999), no. 1, 103–149.
- [MS14] Pierre Mathieu and Alessandro Sisto, *Deviation inequalities for random walks* (2014), available at [arXiv:1411.7865](#).
- [MO15] Ashot Minasyan and Denis Osin, *Acylindrical hyperbolicity of groups acting on trees*, Math. Ann. **362** (2015), no. 3-4, 1055–1105, DOI 10.1007/s00208-014-1138-z. MR3368093
- [MU08] Alexei G. Myasnikov and Alexander Ushakov, *Random subgroups and analysis of the length-based and quotient attacks*, J. Math. Cryptol. **2** (2008), no. 1, 29–61.
- [Osi15] D. Osin, *On acylindrical hyperbolicity of groups with positive first ℓ^2 -Betti number*, Bull. Lond. Math. Soc. **47** (2015), no. 5, 725–730.
- [Osi16] D. Osin, *Acylindrically hyperbolic groups*, Trans. Amer. Math. Soc. **368** (2016), no. 2, 851–888.

- [PS16] Piotr Przytycki and Alessandro Sisto, *A note on acylindrical hyperbolicity of Mapping Class Groups*, Proceedings of the 7th MSJ-SI, Hyperbolic Geometry and Geometric Group Theory, to appear (2016).
- [Riv10] Igor Rivin, *Zariski density and genericity*, Int. Math. Res. Not. IMRN **19** (2010), 3649–3657.
- [Sel97] Z. Sela, *Acylindrical accessibility for groups*, Invent. Math. **129** (1997), no. 3, 527–565.
- [Sis16a] Alessandro Sisto, *Quasi-convexity of hyperbolically embedded subgroups*, Math. Z. **283** (2016), no. 3-4, 649–658.
- [Sis16b] Alessandro Sisto, *Contracting elements and random walks*, Journal für die reine und angewandte Mathematik (Crelle’s Journal), to appear (2016).
- [ST16] Alessandro Sisto and Sam Taylor, *Largest projections for random walks* (2016), available at [arXiv:1611.07545](https://arxiv.org/abs/1611.07545).
- [TT16] Samuel J. Taylor and Giulio Tiozzo, *Random extensions of free groups and surface groups are hyperbolic*, Int. Math. Res. Not. IMRN **1** (2016), 294–310.

Joseph Maher
 CUNY College of Staten Island and CUNY Graduate Center
joseph.maher@csi.cuny.edu

Alessandro Sisto
 ETH Zürich
sisto@math.ethz.ch